UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/672,206	09/28/2000	Danny Raz	5	8786

22046 7590 11/19/2003

LUCENT TECHNOLOGIES INC.
DOCKET ADMINISTRATOR
101 CRAWFORDS CORNER ROAD - ROOM 3J-219
HOLMDEL, NJ 07733

EXAMINER	
KHOSRAVAN, JIMAN	
ART UNIT	PAPER NUMBER
2141	3

DATE MAILED: 11/19/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/672,206	**Applicant(s)** RAZ, DANNY	
	Examiner Jiman Khosravan	**Art Unit** 2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____ .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *9/28/2000* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: .

DETAILED ACTION

Drawing Objections

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: Item 311, figure 3.

A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Appropriate correction is required.

Specification Objections

2. The abstract of the disclosure is objected to because of the length of the abstract.

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details. Correction is required. See MPEP § 608.01(b).

3. The disclosure is objected to because of the following informalities: Page 4, line 13, applicant refers to "Fig. 1, client 104 is shown as being connected to Internet 100 via a router 140 within an Intranet 140." It should read as follows, "Fig. 1, client 104 is shown as being connected to Internet 100 via a router 140 within an Intranet 141."

Appropriate correction is required.

Claim Rejections ~ 35 U.S.C. § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-4 and 8, are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. As per claim 1, the claim recites the limitations "said web guard server" in line 10 and line 12. There is insufficient antecedent basis for these limitations in the claim.

b. As per claim 2, the claim recites the limitations "said process" in line 1. There is insufficient antecedent basis for these limitations in the claim.

c. As per claim 3, the claim recites the limitations “said web guard server” in line 2. There is insufficient antecedent basis for these limitations in the claim.

d. As per claim 4, the claim recites the limitations “said process” in line 4. There is insufficient antecedent basis for this limitation in the claim.

e. As per claim 8, the claim recites the limitations “said packets” in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections ~ 35 U.S.C. § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2 and 5-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Bernhard et al. (US 6,609,205 B1).

a. As per claim 1, Bernhard teaches a method for thwarting coordinated SYN denial of service attacks against a server S disposed in a network of interconnected elements communicating using the TCP protocol, comprising the steps of controlling a network switch to divert a predetermined fraction of SYN packets destined for server, to a web guard processor, establishing a first TCP connection between one or more clients originating the packets and the web guard processor, and a second TCP connection between the client or clients and the server (Fig. 1; Col. 4, lines 12-27: Bernhard discloses an intrusion detection system, IDS, sensor (11) in Fig. 1, capable of examining packets of TCP protocols, located between the external network, the origin of the packet, and router (12), and the internal network (10) where the packet is destined. Bernhard teaches an external network connecting to a router (12) through TCP protocols where a second connection is established between the router (12) and the local network (10). Furthermore, IDS sensor (11) is located in serial with the router (12)). Bernhard further teaches monitoring the number of timed-out connections between web guard server and clients (Col. 7, lines 28-37: Once a SYN event occurs, the process determines whether ACK occurs. If not, the process proceeds to a count). Bernhard also teaches that if the number of timed-out connections between web guard server and the clients exceed a first predetermined threshold, controlling the switch to divert all SYN packets destined to the server to the web guard processor (Sensor (11) contains a detection engine that monitors incoming packets. Once a SYN event occurs, the process determines whether ACK occurs. If the number of SYN packets exceeds 50, all SYN packets are released and misuse is detected: Fig.2; Col. 3, lines 41-52; Col. 6, lines 46-51; Col. 9, lines 5-18).

b. As per claim 2, Bernhard further teaches generating an alarm indicating said server is likely to be under attack (Fig. 2; Col. 3, lines 41-52).

c. As per claim 5, Bernhard further teaches notifying said server that it is under attack (Col. 3, lines 41-52).

d. As per claim 6, Bernhard further teaches notifying other web guard processors in network that server is under attack (Col. 4, lines 38-45).

e. As per claim 7, Bernhard teaches a method for thwarting coordinated SYN denial of service attacks against a server S disposed of interconnected elements communicating using the TCP protocol , where the attack originating from a malicious host generating SYN packets is destined to the server. Bernhard further teaches arranging a switch receiving the SYN packets destined to server and forward them to a TCP proxy arranged to operate without an associated cache, where the TCP proxy, subject to a CSDoS attack, does not successfully establish a TCP connection with the malicious host and no TCP connection is made from the TCP proxy to the server, thereby protecting the server from the attack (Col. 3, lines 41-52; Col. 4, lines 12-27; Col. 7, lines 28-37; Col. 9, lines 5-18).

f. As per claim 8, Bernhard teaches a method for thwarting coordinated SYN denial of service attacks against a server S disposed in a network of interconnected elements communicating using the TCP protocol, comprising the steps of forwarding a statistical sampling of said packets from a switch in said network to a processor, and if the packets in the sampling indicate and attack, altering the operation of the switch to reduce the effects of the attack (Col. 3, lines 41-52; Col. 4, lines 12-27; Col. 7, lines 28-37; Col. 9, lines 5-18).

g. As per claim 9, Bernhard further teaches the switch to be arranged to discard packets in the event an attack is detected (Col. 3, lines 41-52; Col. 4, lines 12-27).

Claim Rejections ~ 35 U.S.C. § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bernhard, and further in view of Sharp et al. (US 2003/0110394 A1).

a. As per claim 3, Bernhard discloses the claimed invention as described above. However Bernhard does not explicitly teach if the number of timed-out connections between the web guard and clients exceed a second predetermined threshold, to delete all SYN packets destined for the server. Sharp discloses a method used to detect and prevent spoofing where when it comes to flooding, there are four (or more or less) threshold levels that exists. Depending on the level of violation, different actions take place by the system. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sharp in the system of Bernhard, because as higher thresholds are violated, the system automatically begins the process of chocking and holding certain packets while sending alarms and notifications to different area in the system. In so doing, the system can dynamically change the amount of choke it places on arriving packets, allowing more during lower thresholds, and declining more during higher threshold violations to allow the system to run more smoothly (Page 1, paragraph [0010]; Page 2, paragraph [0015]; Page 3, paragraphs [0045] & [0048]; Page 4, paragraph [0049]).

b. As per claim 4, Sharp further discloses generating alarms indication the server is under attack (Page 1, paragraph [0010]; Page 2, paragraph [0015]; Page 3, paragraphs [0045] & [0048]; Page 4, paragraph [0049]).

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jinan Khosravan whose telephone number is

(703) 305-0704. The examiner can normally be reached on Monday - Friday from 9:00 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (703) 305-4003. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Communication via Internet e–mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [rupal.dharia@uspto.gov].

All Internet e-mail communications will be made of record in the application file. PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jiman Khosravan
Examiner
Art Unit 2141

November 6, 2003

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER